



Medical Device Security: Where are We Going?



Kevin Fu, Ph.D.

University of Michigan

Director, Archimedes Center for Medical Device Security
Associate Professor, Electrical Engineering & Computer Science
secure-medicine.org kevinfu@umich.edu

**Archimedes:
Safety-Centric
Cybersecurity
Education**



FDA Patient Engagement Advisory Committee, September 10, 2019

Disclosures

- Co-founder, healthcare security startup **VIRTA LABS™**
- Director, Archimedes Center for Medical Device Security
- Fmr. visiting scientist, U.S. Food and Drug Administration
- Consultant to MITRE, Medtronic, and Novartis Pharmaceuticals
- Recent research support:



- Archimedes supported by institutional members





ARCHIMEDES
MEDICAL DEVICE SECURITY
RESEARCH CENTER



Thank You.

I Am The Cavalry



**National Institute of
Standards and Technology**
U.S. Department of Commerce



ECRI Institute
The Discipline of Science. The Integrity of Independence.



My History and Background



VIRTA LABS™



Massachusetts
Institute of
Technology



UMASS
AMHERST



NIST
National Institute
of Standards
and Technology



My opinions are my own and do not necessarily represent or reflect the views of any of my past or current employers

Correctness is easy.

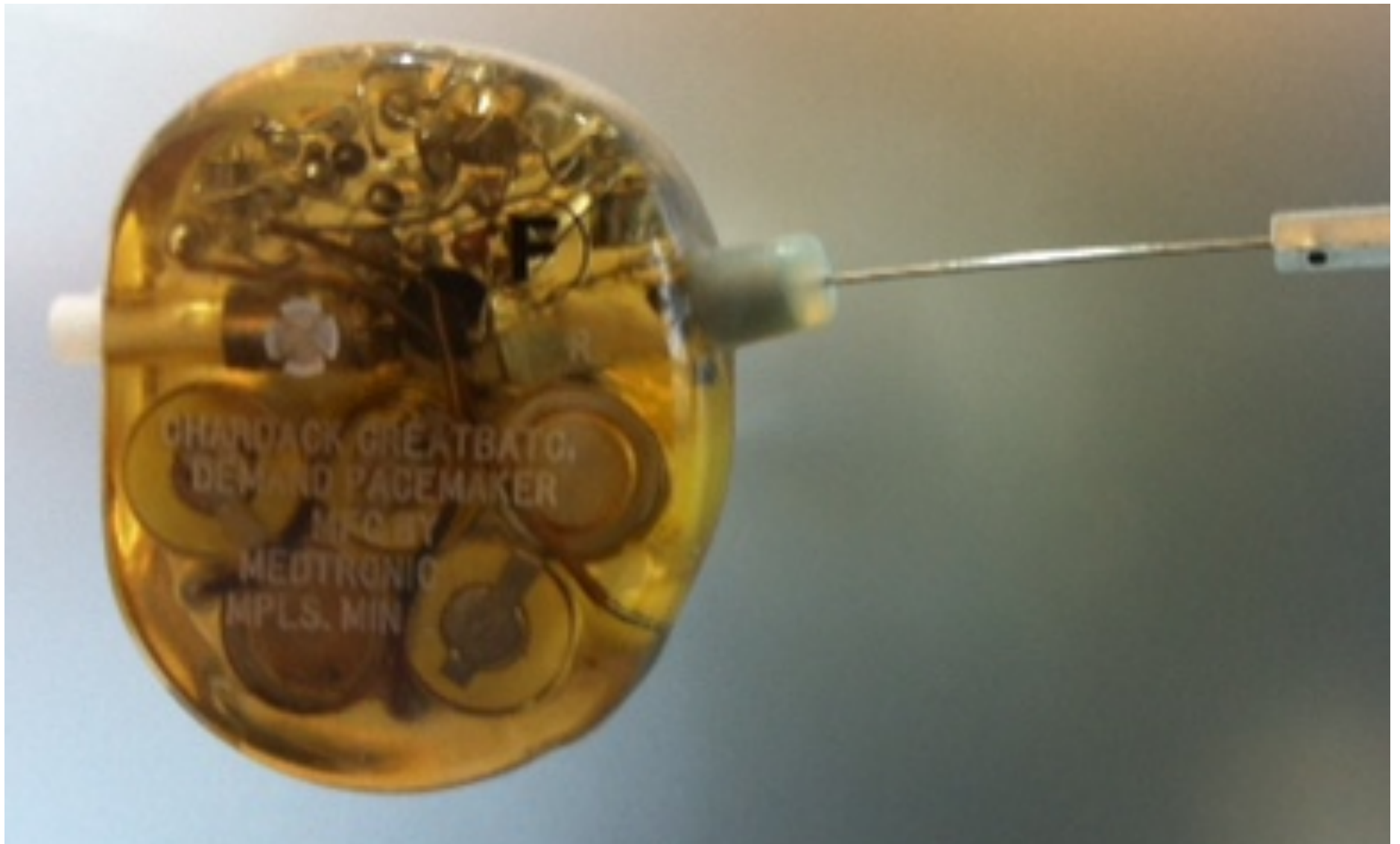


Correctness is easy.

Security is hard.



Wireless medical devices: great benefits. subtle inconvenient risks.



A Photo by Kevin Fu @ Medtronic museum

Medical device sec since 2006...

Invited talk.

Computer system security and medical devices,
U.S. Food and Drug Administration Center for
Devices and Radiological Health (FDA CDRH),
October 2006.



In 2006...

A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY J. FEDER MARCH 12, 2008

The New York Times

Hack: 2008

Of Fact, Fiction and Cheney's Defibrillator

By GINA KOLATA

Published: October 27, 2013

The New York Times

Hype: 2013



Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin[†]
University of Washington

Thomas S. Heydt-Benjamin[†]
University of Massachusetts Amherst

Benjamin Ransford[†]
University of Massachusetts Amherst

Shane S. Clark
University of Massachusetts Amherst

Benessa Defend
University of Massachusetts Amherst

Will Morgan
University of Massachusetts Amherst

Kevin Fu, PhD^{*}
University of Massachusetts Amherst

Tadayoshi Kohno, PhD^{*}
University of Washington

William H. Maisel, MD, MPH^{*}
BIDMC and Harvard Medical School

Abstract—Our study analyzes the security and privacy properties of an implantable cardioverter defibrillator (ICD). Introduced to the U.S. market in 2003, this model of ICD includes pacemaker technology and is designed to communicate wirelessly with a nearby external programmer in the 175 kHz frequency range. After partially reverse-engineering the ICD's communications protocol with an oscilloscope and a software radio, we implemented several software radio-based attacks that could compromise patient safety and patient privacy. Our results show the trade-offs between security and privacy of these devices, based on RF power-centric, bringing patient safety and privacy of their contributions provide potential security and privacy improvements and introduce techniques that address this paper is the first software radios to an communications protocol.

this event to a health care practitioner who uses a *commercial device programmer*¹ with wireless capabilities to extract data from the ICD or modify its settings without surgery. Between 1990 and 2002, over 2.6 million pacemakers and ICDs were implanted in patients in the United States [10]; clinical trials have shown that these devices improve survival [10], but we have not discussed the security of these devices. Without immunity to attacks, the security of these devices is at risk. This paper presents several

Wirelessly reprogrammed (IMDs) such as pacemakers (ICDs), neurostimulators, and implantable cardioverter defibrillators (ICDs) use embedded computers and treat patients with an ICD that senses a rhythm and delivers an electrical shock to restore a normal rhythm.

^{*}Corresponding faculty authors.

- Kevin Fu, Medical Device Security, University of Massachusetts Amherst, Massachusetts 01003
- Tadayoshi Kohno, Medical Device Security, Department of Computer Science and Engineering, University of Washington, Box 352350, Seattle, Washington 98195 (yoshi@cs.washington.edu)
- William H. Maisel, Medical Device Safety Institute, Beth Israel Deaconess Medical Center, Harvard Medical School, 185 Pilgrim Road, Baker 4, Boston, MA 02215 (wmaisel@bidmc.harvard.edu).

Additional information online at <http://www.secure-medicine.org>.

[†]Co-student leads listed in alphabetical order; each participated equally.

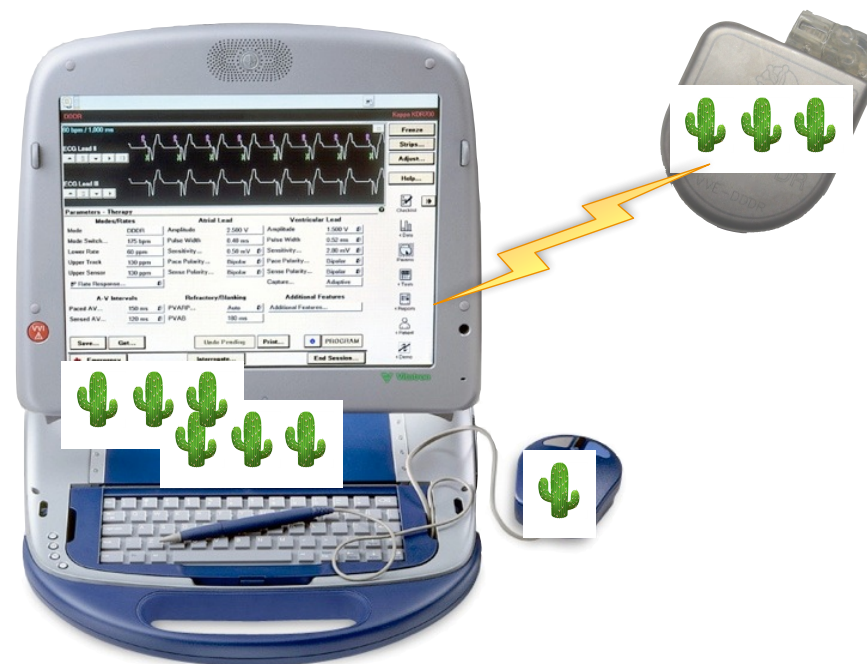
¹The reader should not confuse the term "device programmer" with a person who programs computers. The former is an external device that communicates with and adjusts the settings on an IMD.

This paper, copyright the IEEE, will appear in the proceedings of the 2008 IEEE Symposium on Security and Privacy. 1



Implantation of Defibrillator

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring



Device Programmer

Photos: 🌵🌵🌵; Video: or-live.com

Privacy??

Implanting
physician

Diagnosis

Hospital

Also:
Device state
Patient name

Date of birth
Make & model
Serial no.

... and more

Wirelessly Induce Fatal Heart Rhythm

- 402-405 MHz MICS band, nominal range several meters
- Command shock sends 35 J in ~ 1 msec to the T-wave
- Designed to induce ventricular fibrillation
- No RF amplification necessary



[Halperin et al., IEEE Symposium on Security & Privacy 2008]

Modern Healthcare

THE ONLY HEALTHCARE BUSINESS NEWS WEEKLY | APRIL 11, 2016 | \$5.50

If YOU EVER
WANT TO SEE
YOUR DATA
AGAIN

**Will hospitals
pay for security
to avoid paying up
as ransomware
victims?** Page 8

Hospitals
as venture
capitalists /
Page 12

Rural
hospital
shake-up /
Page 20



npr MICHIGAN RADIO news arts & life music programs

shop



all tech considered TECH, CULTURE AND CONNECTION

PRIVACY & SECURITY

Malware Attacks On Hospitals Put Patients At Risk

April 1, 2016 · 4:34 PM ET

NAOMI LACHANCE



2016



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

[QR Code](#)

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Copy

Check Payment

Decrypt

Powerful Russian Orthodox cleric summoned to spritz computers with holy water to fight ransomware



← Ways Forward ↗

Security should
be **designed** in

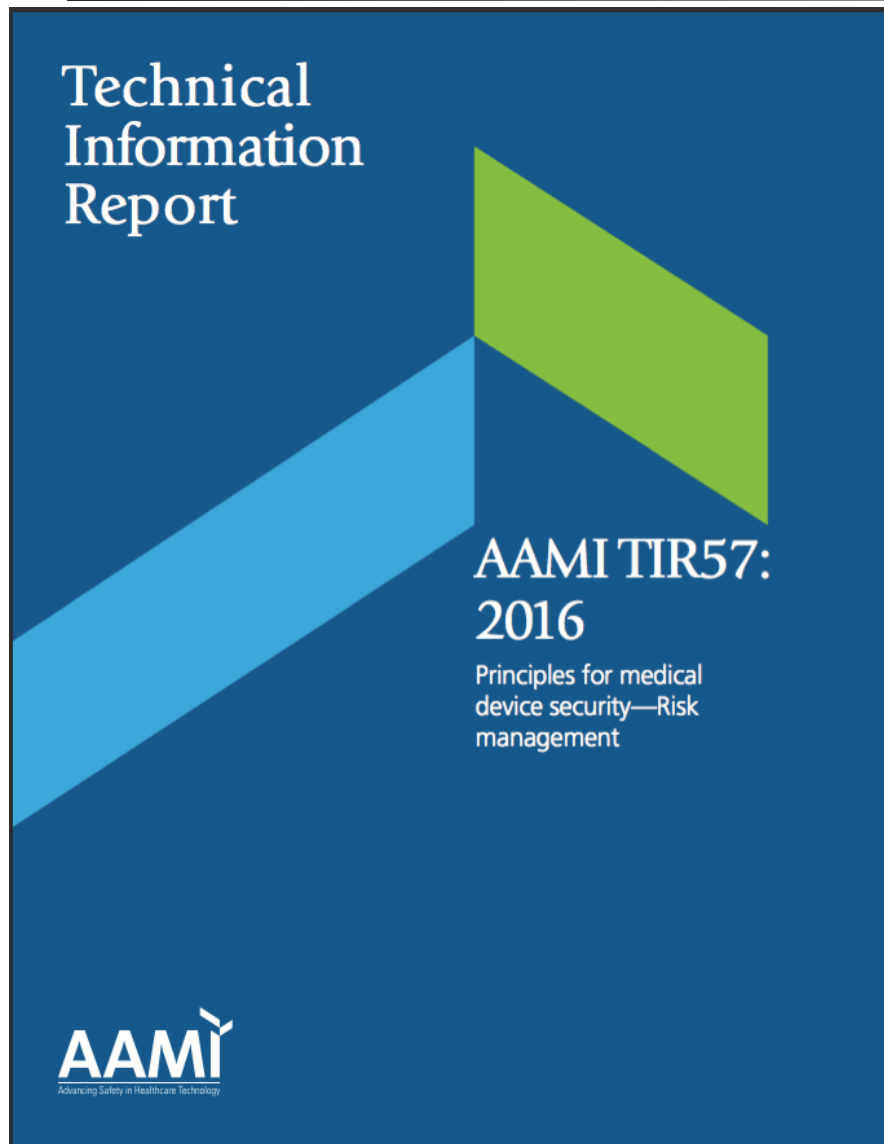


not **bolted** on



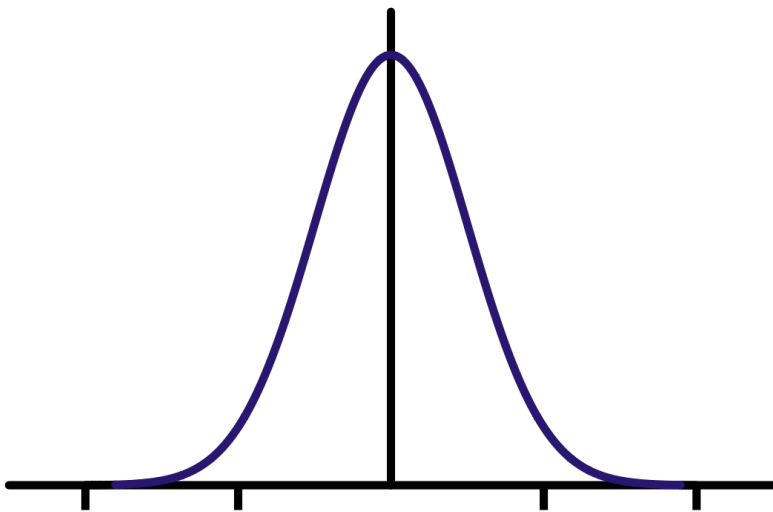
AAMI TIR57: Premarket Engineering

- Principles of medical device security risk management



Safety :: Security

- Safety: Probability distribution normal, mother nature
- Security: Adversary causes the unsafe 1% to be 100%



VS.



Vulnerability Disclosure & Incidents

- Caution: Victim blaming vendors, manufacturers, HDOs
- Meaningful questions to ask:
 - How will medical devices **fail gracefully** when under attack?
 - What mitigating security controls are **designed into** medical devices to continue to function safely **even if hacked**?
 - ~~Is our medical device hackable?~~
 - ~~Has our medical device been hacked?~~
 - ~~Will our medical device be hacked?~~

Cybersecurity: Patients First

- Biggest risk at the moment:
 - Hackers ~~breaking into medical devices~~
 - Wide-scale **unavailability** of patient care
 - **Integrity** of medical sensors
- Gaps
 - **Procurement:** HDOs build cybersecurity into contract requirements (e.g., Mayo Clinic vendor book)
 - **Clinical Operations Cybersecurity:**
Know your assets cyber risk (e.g., my company Virta Labs)
 - Prioritizing to **clinically relevant** cybersecurity risks. Safety first.
- Challenges
 - Don't interrupt clinical workflow
 - Many security specialists focus on technical controls
 - Many safety specialists focus on risk management



Reference Slides

Related Publications

- "Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory" by D. Kramer, K. Fu, JAMA, October 18, 2017 <https://jamanetwork.com/journals/jama/fullarticle/2659246>
- "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists" by B. Ransford et al. PACE, July 2017 <http://onlinelibrary.wiley.com/doi/10.1111/pace.13102/abstract>
- "Hospitals Need Better Cybersecurity, Not Fear" by Fu et al., Modern Healthcare, September 2016 <http://www.modernhealthcare.com/article/20160914/NEWS/160919950>
- "On the Technical Debt of Medical Device Security" by K. Fu, National Academy of Engineering FOE, September 2015. <https://www.naefrontiers.org/File.aspx?id=50750>
- "Inside Risks: Controlling for Cybersecurity Risks of Medical Device Software" by K. Fu, J. Blum. CACM, October 2013 <http://www.csl.sri.com/users/neumann/cacm231.pdf>
- "Trustworthy Medical Device Software" by K. Fu. In Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report, Washington, DC, July 2011. IOM (Institute of Medicine) <https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf>
- "Reducing the Risks of Implantable Medical Devices: A prescription to improve security and privacy of pervasive health care" by K. Fu, CACM 52(6), June 2009. <http://www.csl.sri.com/users/neumann/insiderisks08.html#218>
- "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" by D. Halperin et al. In IEEE Symposium on Security and Privacy, May 2008. <https://www.secure-medicine.org/public/publications/icd-study.pdf>

Modern Healthcare



Commentary: Hospitals need better cybersecurity, not more fear

By Kevin Fu, Dr. John Halamka, Jack Kufahl and Mary Logan | September 14, 2016

We've seen unprecedented attention to medical-device security after an **unorthodox report** was recently released by short-selling investment research firm Muddy Waters Capital and MedSec, which alleged security vulnerabilities in **St. Jude Medical's** pacemakers. An **independent research team** subsequently raised doubts about some of the clinical claims made by the report. St. Jude Medical, meanwhile, has filed a lawsuit disputing the allegations in the same report.

Cybersecurity and medical devices: A Practical guide for cardiac electrophysiologists

Benjamin Ransford PhD, Daniel B. Kramer MD, MPH, Denis Foo Kune PhD, Julio Auto de Medeiros, Chen Yan, Wenyuan Xu PhD, Thomas Crawford MD, Kevin Fu PhD

Accepted manuscript online: 17 May 2017 [Full publication history](#)

VIRTA LABS™



Making Sense of Muddy Waters & MedSec

Industry White Paper
September 1, 2016 (Updated April 18, 2017)
info@virtalabs.com

Public Release
Copyright 2017 Virta Laboratories, Inc.
All rights reserved.

Ransomware: How we can climb out of this mess

Privacy & Security

Healthcare security experts argue that hospitals must ensure high availability of medical devices and IT systems with practices that resemble preventing and treating disease. Because ransomware is a symptom rather than the problem.

By **Kevin Fu and Harold Thimbleby** | June 05, 2017 | 07:04 AM



Join ACCE at AAMI 2017!

See **Slide 2** for more details

President's Message

Dear members and colleagues,

It is a pleasure to welcome you to the 2017 ACCE meeting. This year's theme is "Cybersecurity and Medical Devices". The meeting will focus on the latest developments in this field, with a particular emphasis on the challenges faced by clinicians and researchers. The meeting will be held at the AAMI 2017 conference, which is a great opportunity to learn from the experts and to share your own experiences.

The meeting will be held at the AAMI 2017 conference, which is a great opportunity to learn from the experts and to share your own experiences.